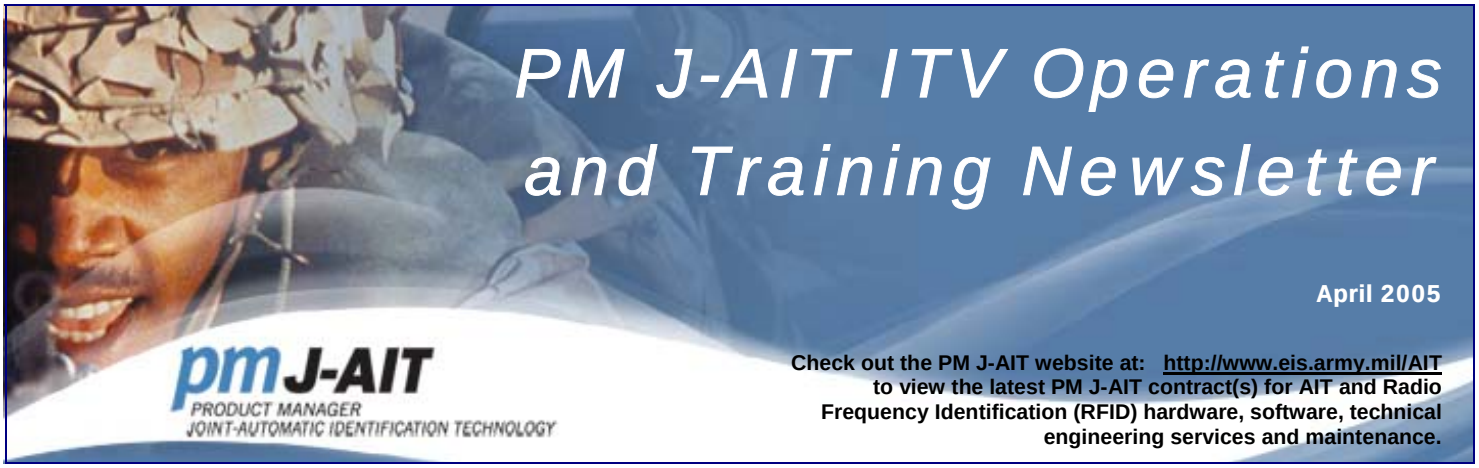


PM J-AIT ITV Operations and Training Newsletter

April 2005

pmJ-AIT
PRODUCT MANAGER
JOINT-AUTOMATIC IDENTIFICATION TECHNOLOGY

Check out the PM J-AIT website at: http://www.eis.army.mil/AIT to view the latest PM J-AIT contract(s) for AIT and Radio Frequency Identification (RFID) hardware, software, technical engineering services and maintenance.

Analyzing Blank RFID Tags

Approximately one month ago, the Combined Arms Support Command (CASCOM) In-Transit Visibility (ITV) representatives were contacted by the Surface Deployment and Distribution Command (SDDC) to do a data comparison on a Third Infantry Division (3ID) unit movement from Fort Stewart, GA to theater, comparing data from the National (CONUS) ITV Server with the Worldwide Port System (WPS). The analyses of the 3ID deployment required data collection from a variety of RF-ITV read and write sites, both in theater and CONUS. The information collected began to show trends within the data. For instance, we noted an inordinate number of "blank tags" (tags with no license plate, commodity, or TCMD data) at Ash Shuaibah, Kuwait. This was not directly related to the initial undertaking of tracking the 3ID deployment; however, it did peak our interest to find out why so many blank tags were moving through the distribution system.

Coming in the May issue of the PM J-AIT ITV Operations and Training Newsletter…more on the 3ID Unit Move analysis.

Solving the mystery…

We began by extracting the tags read at Shuaibah into an Excel spreadsheet for data analysis (see page 40 of the *latest ITV Server Guide (the green booklet)* or the August 2005 edition of the *PM J-AIT ITV Operations and Training Newsletter* for instructions on how to extract ITV server data into Excel). Various Excel sorts were used on the extracted data to determine trends and/or groupings of tags. The patterns or trends we were looking for included: blocks/groups of blank tag ID numbers in sequence; a block/group of blank tags being first seen or last seen by a particular read interrogator within a compressed time frame (indicating a convoy or rail movement); and a written (or populated) tag amongst a sequential group of blank tags possibly providing write data to indicate an origin for the sequenced group. This was where the real Sherlock Holmes work began… and it's not so elementary dear Watson!

One such pattern/group of blank tags led us to the read interrogator described as CHARLESTON SC TC DOCK RAIL (refers to the registered interrogator description). Research indicated that hundreds of sequentially numbered blank tags were being first read at the Charleston rail interrogator during the months of December 2004 and January 2005. These hundreds of tags provided no license plate or commodity detail. The only information that could be determined from the read event status was where and when the tags were first seen, the route they followed, and where/when the tags stopped moving or when they reached their final destination.

Using the Excel sorting functions, we were able to determine when trains or truck convoys carrying groups of blank tags arrived at the Charleston Railhead Truck Gate and were originating from one location. We expanded the time frame of our data selection to see if we could establish when the blank tags first started arriving at Charleston and if blank tags

If you have any questions or comments, please contact the following points of contact:

Quality Assurance ITV Server

Ralph Ocasio
RF-ITV Operations Section Lead
ralph.ocasio@us.army.mil
(703) 339-4400 ext. 104

Jerry Rodgers
Operational Readiness
jerry.d.rodgers@us.army.mil
(703) 339-4400 ext. 112

Kathy Flowers
CONUS & PACOM Operational Readiness
Kathy.bonds1@us.army.mil
(703) 339-4400 ext. 117

Harry Meisell
CENTCOM/NATO
harry.meisell@us.army.mil
(703) 339-4400 ext. 124

Tom Rigsbee
EUCOM
Thomas.Rigsbee@us.army.mil
49-170-978-6540

TIPS/ITV Server Training

Richard Mack
rmack4@csc.com
(804) 863-2485 ext. 205

Sherman Duncan
sduncan@lesco-logistics.com
(804) 863-2485 ext. 206

Bob Wendt
robert.m.wendt.lsg@lee.army.mil
(804) 734-1692 (DSN 687)

If this newsletter has been forwarded to you and you would like to be added to the distribution list, please send your request via E-mail to PM J-AIT (Jerry Rodgers) at jerry.d.rodgers@us.army.mil.

were still arriving there. Combining and sorting the new October/November tag data with the previously extracted December/January tag data, led us to sequentially lower-numbered tags. In addition, it provided tags with read events prior to Charleston, license plate data, and finally a write event status which indicated who wrote the tag.

2005 ITV Server Guide and 2005 RFID Operations Guide:
http://www.cascom.army.mil/Automation/ITV/index.htm

TIPS Write and Read Operations Tutorial:
https://highland.rfitv.army.mil/TT/

ITV Servers:
National (CONUS): https://highland.rfitv.army.mil
Europe: https://itv.aelog.army.mil
Pacific: https://usfkitv.korea.army.mil
Southwest Asia: https://cenitv1.arifjan.arcent.army.mil
Training: https://trainer.rfitv.army.mil

Using the write site registration information of the National (CONUS) ITV Server, we contacted the Point of Contact (POC) at the O'Gara-Hess & Eisenhardt, a U.S. Army vendor for vehicle armor. A quick discussion revealed that approximately 500 up-armored High Mobility Multipurpose Wheeled Vehicles (HMMWVs) per month were the items being shipped with blank tags. Throughout October and November, O'Gara-Hess wrote RFID tag data for the HMMWVs and uploaded the tag data to the National ITV Server. On 29 November 2004, their write station computer was relocated and the IP address changed, breaking connectivity to the National ITV Server. Not knowing who to contact to re-establish connectivity to continue writing RFID tags and uploading the data, the decision was made to continue attaching tags (although blank) to the HMMWVs traveling through the distribution system. On 29 January 2005, O'Gara-Hess ran out of RFID tags/batteries and started shipping 500 up-armored vehicles per month with no tags at all—not even blank tags.

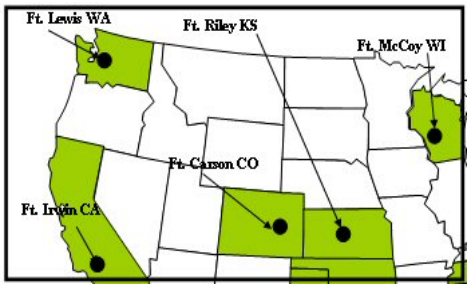
The bad news is that approximately 900 HMMWVs were shipped with blank tags during December/January and over 1000 were shipped during February/March without any tags. The good news is that PM J-AIT has made contact with O'Gara-Hess and is upgrading their tag writing software, reestablishing connectivity with the National ITV Server, and establishing a tag/battery redistribution issue program to ensure long term availability of tags at this manufacturer's site.

Impact of Blank Tags

Blank tags moving through the system negate the ability to search for particular items/shipments when doing ITV server queries. Blank tags also make it impossible to determine the shipment's origin/designation, not to mention the container's contents. So if you plan on tracking your deployment, unit sustainment, or doing your own analysis, it is important to verify that your tags have been written and uploaded correctly to the proper ITV server by performing a quick query on the ITV server. If you are returning tags for reissue, make sure the tags have been erased and the batteries have been turned around to deactivate the tags. For retrograde equipment, make sure you have written your tags and uploaded the data by performing a quick ITV server query.

During our data collection and analysis, we found trends/patterns of additional blank tags from other locations moving through the system. We decided to concentrate on the blank tag issue for the next 90 days and will present the initial data in a future edition of this newsletter. We focused on 30 days worth of data on CONUS sites between 1 March 2005 and 15 April 2005. We divided the sites within four outlined regions and had ITV analysts from CASCOM use the *RF Interrogator and Multiple Data Elements* query on the National ITV Server to conduct a data analysis on various Army, Air Force, Marine, and Defense Logistics Agency (DLA) sites.

NORTHWEST REGION



Sites viewed in this region were Fort Lewis, WA; Fort Carson, CO; Fort Irwin, CA; Fort Riley, KS; Fort McCoy, WI; and a port in Tacoma, WA.

The following sites indicated a trend/pattern of blank tags:

SITE	TOTAL TAGS	TOTAL BLANK TAGS
FORT LEWIS, WA	2878	211
FORT CARSON, CO	91	16

Fort Lewis, WA

Finding: Analysis indicated that blank tags were not originated by Fort Lewis but rather from Fort Wainwright, AK.

Corrective Action: The CASCOM will expand the analysis to Fort Wainwright, AK to see if there is a trend/pattern of blank tags at Fort Wainwright or if the problem is traceable to another location.

Fort Carson, CO

Finding: Analysis indicated that blank tags were not originated by Fort Carson but were retrograde tags returning from the Central Command (CENTCOM) Area of Responsibility (AOR).

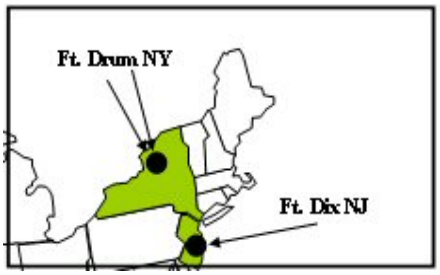
Corrective Action: It is recommended that all retrograde tags be erased and the batteries be inverted to deactivate the tags prior to returning them. If returning retrograde equipment, ensure that tags are written with pertinent data and uploaded to the correct ITV server before shipping. The tracking and return of equipment/reparables is an important step in refurbishing the force.

NORTHEAST REGION

Sites viewed in this region were Fort Drum, NY; Fort Dix, NJ; Dover AFB, NJ; McGuire AFB, NJ; and Mechanicsburg, PA

The following sites show a trend/pattern of blank tags:

SITE	TOTAL TAGS	TOTAL BLANK TAGS
DOVER AFB, DE	6308	510
MCGUIRE AFB, NJ	1164	41
MECHANICSBURG, PA	651	87
FORT DRUM, NY	198	68
FORT DIX, NJ	196	19



Dover AFB, DE

Finding: Out of the 510 total blank tags, 170 were in the 4 and 5 million serial number range. The 170 blank tags were tracked back to an origination point of the San Francisco Fed Ex cargo site which were then shipped to Dover AFB then to New Cumberland and then into the CENTCOM AOR. Based on the serial number sequence, it was determined that these are new tags.

Corrective Action Taken: Since they do not track orders for tags by serial number, New Cumberland was unable to identify who the tags were issued to. The RFID tag manufacturer, Savi, has confirmed that these tags were new tags, bought by the DLA and shipped via Dover AFB for use by customers in the CENTCOM AOR. The CASCOM will expand the analysis to determine any trends for the remainder of the blank tags.

Mechanicsburg, PA

Finding: Of the blank tags, 14 were in the 4 million series. Thirteen were found between New Cumberland and Mechanicsburg, and one was from Tracy. All other tags were either retrograde from the CENTCOM AOR or from the other CONUS DLA sites.

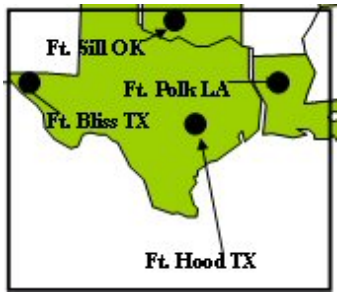
Corrective Action Taken: It is recommended that all retrograde tags be erased and the batteries be inverted to deactivate the tag prior to returning them. If returning retrograde equipment, ensure that tags are written with pertinent data and uploaded to the correct ITV server before shipping. The tracking and return of equipment/reparables is an important step in refurbishing the Force. The CASCOM will expand the analysis to determine any trends at New Cumberland or other CONUS DLA sites.

Fort Drum, NY/Fort Dix, NJ/McGuire AFB, NJ

Finding: Analysis indicated that blank tags were not originated by Fort Drum, Fort Dix, or McGuire AFB but were retrograde tags returning from the CENTCOM AOR.

Corrective Action: It is recommended that all retrograde tags be erased and the batteries be inverted to deactivate the tags prior to returning them. If returning retrograde equipment, ensure that tags are written with pertinent data and uploaded to the correct ITV server before shipping. The tracking and return of equipment/reparables is an important step in refurbishing the force.

SOUTHWEST REGION



Sites viewed in this region were Fort Sill, OK; Fort Polk, LA; Fort Bliss, TX; and Hood, TX.

The following sites show a trend/pattern of blank tags:

SITE	TOTAL TAGS	TOTAL BLANK TAGS
FORT HOOD, TX	848	127
FORT POLK, LA	531	63
FORT BLISS, TX	164	13

Fort Hood, TX

Finding: Of the total number of blank tags, 31 of the tags had been erased and then sent, by way of Gray Army Air Field, back to the CENTCOM AOR. Of the total number of blank tags, 8 tags were seen using Fort Hood at a rail switching point for further transfer to Fort Lewis and Portsmouth. The remaining tags that showed up at Fort Hood were retrograde coming back from CENTCOM AOR.

Corrective Action Taken: The tracking and return of equipment/reparables is an important step in refurbishing the force. Fort Hood's Installation Transportation Officer (ITO) was notified of the problem and sent a spreadsheet for corrective action. During the remainder of the 90-day campaign to look at blank tags, a follow-up analysis will be performed to determine permanency of corrective action. It is recommended that all retrograde tags be erased and the batteries be inverted to deactivate the tags prior to returning them. If returning retrograde equipment, ensure that tags are written with pertinent data and uploaded to the correct ITV server before shipping.

Fort Polk, LA

Finding: Of the blank tags, 11 tags were found to have come from Fort Drum in early February 2005 and then sent back (blank) to Fort Drum in April as a one-time occurrence. No pattern or trend was identified. The remainder of blank tags was retrograde from the CENTCOM AOR.

Corrective Action Taken: It is recommended that all retrograde tags be erased and the batteries be inverted to deactivate the tags prior to returning them. If returning retrograde equipment, ensure that tags are written with pertinent data and uploaded to the correct ITV server before shipping. The tracking and return of equipment/reparables is an important step in refurbishing the force.

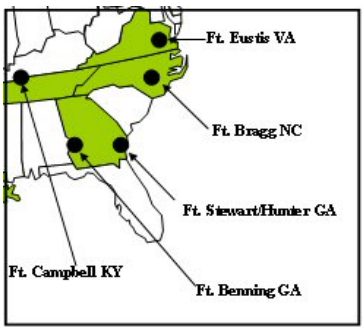
Fort Bliss, TX

Finding: No trend was noted for Fort Bliss. The 13 blank tags found did not originate at Fort Bliss. Nine (9) were sent from Fort Wainwright, AK and four (4) from Fallbrook, CA Naval Weapons Station.

Corrective Action Taken: CASCOM will expand the analysis to Fort Wainwright, AK and Fallbrook, CA Naval Weapons Station to see if there is a trend/pattern of blank tags at these locations or if the problem is traceable to another location.

SOUTHEAST REGION

Sites viewed in this region were Fort Eustis, VA; Fort Bragg, NC; Pope AFB, NC; Camp Lejeune, NC; Fort Benning, GA; Fort Stewart, GA; Hunter AFB, GA; and New River, NC.



The following sites show a trend/pattern of blank tags:

SITE	TOTAL TAGS	TOTAL BLANK TAGS
MCAS NEW RIVER, NC	253	174
CAMP LEJEUNE, NC	1180	176
FORT EUSTIS, VA	266	145
FORT BRAGG, NC	889	48
POPE AFB, NC	148	28
FORT STEWART, GA	121	13

New River, NC

Finding: The analysis indicated trends/grouping of blank tags originating at Marine Corps Air Station (MCAS) New River and MCAS Cherry Point. Data indicated that blank tags are on staged equipment scheduled for future movement/deployment. Additionally, a "ping-pong" (back and forth reading between two interrogators) was noted at NEW RIVER NC MCAS MAIN GATE and NEW RIVER NC MCAS GATE 2.

Corrective Action Taken: The batteries should be inverted in the tags on the staged equipment or items should be moved beyond the interrogation range until cargo is scheduled for movement. After contacting the RFID infrastructure POC, the number of blank tags decreased to 17 tags. During the remainder of the 90-day campaign to look at blank tags, a follow-up analysis will be performed to determine constancy of corrective action. In addition, the Savi Field Service Engineer (FSE) was contacted to investigate the "ping-pong" issues.

Camp Lejeune, NC

Finding: Analysis indicated trends/groupings of blank tags that originated from Camp Lejeune. Of the total number of blank tags, 37 tags went from Lejeune gates to the Charleston Ocean Terminal; 14 tags went from Lejeune to Cherry Point then on to the Al Asad Flight Line; and 70 of the blank tags were read one time on 21 March 2005 at Piney Green gate and not read again (these could be unattached tags in boxes). Fifteen blank tags were returns from the CENTCOM AOR.

Corrective Action Taken: The CASCOM ITV Training Team traveled to Camp Lejeune and provided training on RFID tag writing procedures and the ITV server to Marines from Force Service Support Group (FSSG) Rear on 27 and 28 April 2005. It is recommended that all retrograde tags be erased and the batteries be inverted to deactivate the tags prior to returning them. If returning retrograde equipment, ensure that tags are written with pertinent data and uploaded to the correct ITV server before shipping. The tracking and return of equipment/reparables is an important step in refurbishing the force.

Fort Eustis, VA

Finding: Analysis indicates the majority of the blank tags started at Fort Eustis. Twenty blank tags departed Fort Eustis and went to the Charleston Ocean Terminal. The remainder of the blank tags consisted of training tags used during the Bull Run Exercise at the Transportation School. Of the total number of blank tags, 21 were tags returned from the CENTCOM AOR.

Corrective Action Taken: The Fort Eustis POC has been contacted to discuss 20 blank tags departing Fort Eustis. To support the RFID training objectives of the Transportation School, modifications were made in a collaborative effort between the school, PM J-AIT, and Unisys as to how tags used during the Bull Run Exercise would appear as blank tags on the National ITV Server and populated tags on the ITV Training Server. It is recommended that all retrograde tags be erased and the batteries be inverted to deactivate the tags prior to returning them. If returning retrograde equipment, ensure that tags are written with pertinent data and uploaded to the correct ITV server before shipping. The tracking and return of equipment/reparables is an important step in refurbishing the force.

Fort Bragg, NC

Finding: The majority of blank tags appear to be moving around Fort Bragg--either attached to vehicles or consolidated in a box or crate. A trend was noted where multiple tags provided the same date/time read event(s) indicating that they were batched together. Additionally, a portion of the tags were found to have been retrograded from the CENTCOM AOR during the summer of 2004, and apparently the batteries were not inverted to turn the tag off.

Corrective Action Taken: The tag information was provided to the site Unit Movement Coordinator (UMC) for further coordination with the Ammunition Supply Point (ASP) and Central Receiving Point (CRP) to invert all batteries and return to the UMC for reuse. During the remainder of the 90-day campaign to look at blank tags, a follow-up analysis will be performed to determine permanency of corrective action.

Pope AFB, NC

Finding: Analysis indicated that all blank tags were not originated by Pope AFB but were retrograde tags returning from the CENTCOM AOR.

Corrective Action Taken: It is recommended that all retrograde tags be erased and the batteries be inverted to deactivate the tags prior to returning them. If returning retrograde equipment, ensure that tags are written with pertinent data and uploaded to the correct ITV server before shipping. The tracking and return of equipment/reparables is an important step in refurbishing the force.

Fort Stewart, GA

Finding: Analysis indicated that blank tags were not originated by Fort Stewart but were retrograde tags returning from the CENTCOM AOR.

Corrective Action Taken: It is recommended that all retrograde tags be erased and the batteries be inverted to deactivate the tags prior to returning them. If returning retrograde equipment, ensure that tags are written with pertinent data and uploaded to the correct ITV server before shipping. The tracking and return of equipment/reparables is an important step in refurbishing the force.

How Blank Tags Occur

Tags with no license plate data, or blank tags, occur when:

1. Unpopulated tags are placed on cargo, containers, or equipment scheduled for movement.
2. Tags are erased for return or reissue but the battery is not turned around to deactivate the tags--while they continue to move through the system.
3. Populated tags are not uploaded to the server.
4. **There are no Quality Assurance (QA) checks on the ITV server to ensure data is uploaded to the ITV server; and when there is a lack of ITV training.**
5. Tags are populated, but uploaded to the ITV Training Server instead of the National ITV Server. Items or shipments begin to move through the distribution pipeline and are read by interrogators which upload the tag events to the ITV servers.
6. Tags held for reuse or return are placed/staged within range of an interrogator and are being read—this will also degrade battery life.

Additional Noted Issue:

A concern which surfaced during our analysis of the 3ID deployment was that tagged equipment was moving from a Fort Benning write station directly to the Point of Embarkation (POE) in Savannah without being read by any interrogators in between. There should be interrogators reading the tags at the Fort Benning rail exit. PM J-AIT recommends a site survey be done to ensure adequate interrogator coverage at this site.

Good news story: We found during our analysis that RFID tags are being sent back from the CENTCOM AOR for reuse. Now we need to instill the discipline required to ensure that data for retrograde equipment is written and uploaded to the correct ITV server--and if only the tags are being retrograded for reuse, they are erased and have their batteries inverted to deactivate them.

Another Mystery Solved

Camp Shelby, MS was one of the locations that were identified during out 3ID analysis as having a small problem of blank tags leaving the installation. Using the ITV server registration information for the Camp Shelby write sites, we were able to contact the site's POC to discuss the blank tags.

We recommend that you periodically check your ITV registration POC information for accuracy.

Viewing the registration information, it was noted that their write stations had been improperly registered to the ITV Training Server rather than the National ITV Server. In addition, they were using an outdated version of RFID write software. Correcting the outdated RFID write software was an easy fix; however, the registration to the Training ITV Server could cause a problem for Camp Shelby writing tags. This improper registration to the Training ITV Server meant that for any tags written, the license plate, commodity data, TCMD data, and the initial write event data only would be uploaded to the ITV Training Server--**NO** tag data/information would be seen on the National ITV Server. Therefore, as Camp Shelby's tagged equipment moves through the distribution pipeline and is read by the ITV interrogators, the National ITV Server would display read events (date/time seen) against a supposedly blank tag.

Completing tag data and upload QA checks on the ITV Server is paramount!

To correct the problem, the Camp Shelby transportation technician was first guided through the RFID software download/installation procedures and then through the process for changing site registration to the National ITV Server where it belonged. A very simple and quick process.

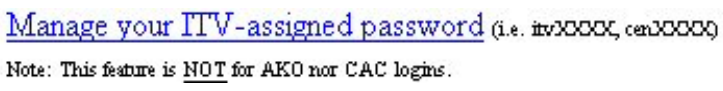
For more information/guidance on site registration see the Nov/Dec 2004 issue of PM J-AIT ITV Operations and Training Newsletter at:

http://www.cascom.army.mil/Automation/ITV/index.htm

With the write software now updated and the registration problem corrected, Camp Shelby is ready to properly write and upload tags. The timing for these corrections couldn't have been better, because Camp Shelby is expecting to get a lot of business this coming year with units deploying through that installation. During the May-June time frame, they are expecting to write approximately 450 tags. Now we'll have ITV on the deploying equipment rather than merely tracking 450 blank tags. Additionally, with a planned mobilization of a Brigade-size unit through Camp Shelby over the next year, who knows how many thousands of blank tags will be avoided?

Manage Your ITV-Assigned Password

You can now manage your ITV-assigned password on-line. Users can update their passwords via the National ITV Server (https://highland.rfitv.army.mil). This update feature is not for AKO or CAC passwords and is only available on the National ITV Server.



From and For the Field…

Lessons Learned at Friedrichsfeld Depot, GE

When Field Service Engineers (FSEs) installed TIPS Read V3.5.1.42 at the main gate of Friedrichsfeld Depot, GE, the interrogation cycle drastically increased from the normal 8-10 seconds to instances of over 1.5 minutes and a norm of about 27-30 seconds. When this was discovered, FSEs knew they would have a problem trying to hit RF-tagged shipments as cargo entered or departed through the main gate node. Senior Field Service Engineer, Dan Goodspeed and Savi Engineer, Bruno Skracic coordinated efforts to identify the source of the problem and began to formulate a solution. In an effort to correct the interrogation problem, a Model 650 was installed to replace the Model 410 which improved the interrogation cycle. In addition to the problem of the interrogation cycle, it was found that the main gate had been experiencing RF interference. It was determined the source of the RF interference was coming from the Wireless Network Access Points the German trucking firm located next door was using for their bar code readers. The problem was going to be constant, and moving the equipment to different locations along the route had little or no impact on decreasing the level of interference. To deal with the interference and minimize its impact on the collection of RF-tagged equipment and shipments as they passed through the main gate, an RF interference shield was constructed and installed. Congratulations to Dan and Bruno on locating the source of problems and their resourcefulness in solving them!

For more details on this operation, contact Tom Rigsbee, PM J-AIT Liaison to USAREUR G4 at Thomas.Rigsbee@hq.hqusareur.army.mil.

RF interference solution at Friedrichsfeld Depot, GE

Bad Tag? Maybe Not!

Some RFID tags previously thought to be “bad” tags may really be good. In some cases, the black rubber cover or plug on the docking station connection port (*see photo*) was not placed into the port or comes loose during shipment exposing the contact points to the elements. When contact points are exposed they can become dirty affecting the ability to write to the tag which may cause the user to assume the tag is bad. For corrective action, it is recommended that you use a cotton swab with alcohol to remove the dirt from the contact points. For preventative action, ensure that docking station connection port cover is properly and tightly inserted into the port.